

ABSTRACT

5 This invention provides a method for accelerating multiplication of an elliptic curve point $Q(x,y)$ by a scalar k , the method comprising the steps of selecting an elliptic curve over a finite field F_q where q is a prime power such that there exists an endomorphism ψ , where $\psi(Q) = \lambda \cdot Q$ for all points $Q(x,y)$ on the elliptic curve; and using smaller representations k_i of the scalar k in combination with the mapping ψ to compute the scalar multiple of the elliptic curve point Q .

0931013 081701
T0280"ET0E60